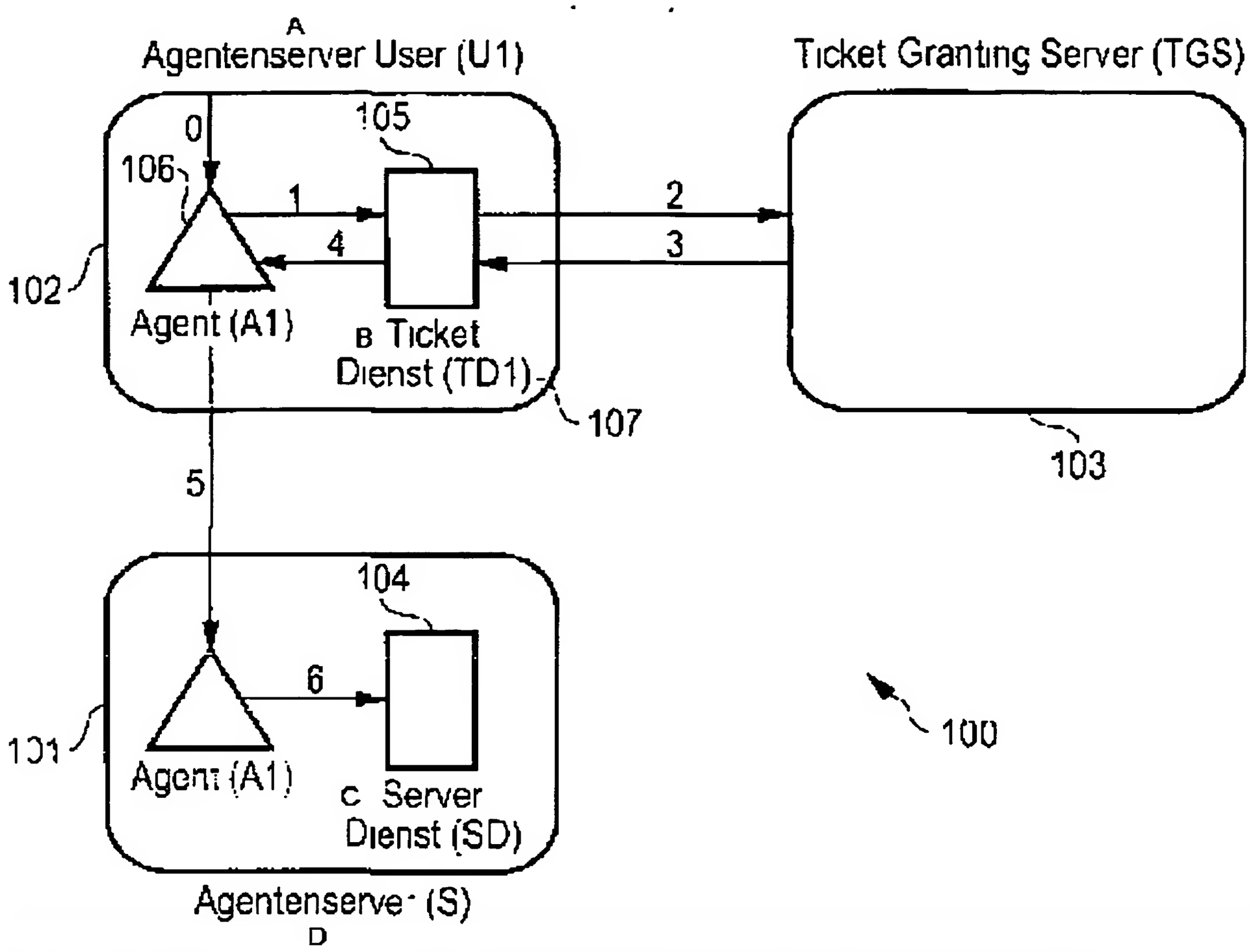
(4)

AN: PAT 2003-833818
TI: Mobile agent authorization method for use in a communications network, whereby an authorization authority processes an authorization request and generates authorization data so that the agent can access a service
PN: WO2003088012-A1
PD: 23.10.2003
AB: NOVELTY - Method for authorization of a mobile agent in a communications network to access a service offered in the communications network, where the agent is an independent, autonomous computer program used to access said service. An authorization request is made to an authorization authority in the communications network, which authorizes access of the mobile agent to the service. The request is verified by the authority, which generates authorization data accordingly. The data is furnished to the agent to allow it to access the service. DETAILED DESCRIPTION - The invention also relates to a corresponding authorization arrangement and computer program product.; USE - Authorization of a mobile agent in a communications network, e.g. for use in providing tickets online. ADVANTAGE - A finely granulated system and task specific authorization of agents can be implemented in a simple fashion. DESCRIPTION OF DRAWING(S) - The figure shows authorization of an agent according to the invention. The system shown is for an online ticket server to which agents or users connect for the issuing of a service, in this case a ticket.
PA: (SIEI) SIEMENS AG;
IN: FISCHER K; LOTZ V; WAIDELICH F;
FA: WO2003088012-A1 23.10.2003; AU2003232596-A1 27.10.2003; **DE10215746**-A1 06.11.2003;
CO: AE; AG; AL; AM; AT; AU; AZ; BA; BB; BE; BG; BR; BY; BZ; CA; CH; CN; CO; CR; CU; CY; CZ; DE; DK; DM; DZ; EA; EC; EE; ES; FI; FR; GB; GD; GE; GH; GM; GR; HR; HU; ID; IE; IL; IN; IS; IT; JP; KE; KG; KP; KR; KZ; LC; LK; LR; LS; LT; LU; LV; MA; MC; MD; MG; MK; MN; MW; MX; MZ; NI; NL; NO; NZ; OA; OM; PH; PL; PT; RO; RU; SC; SD; SE; SG; SI; SK; SL; SZ; TJ; TM; TN; TR; TT; TZ; UA; UG; US; UZ; VC; VN; WO; YU; ZA; ZM; ZW;
DN: AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG; BR; BY; BZ; CA; CH; CN; CO; CR; CU; CZ; DK; DM; DZ; EC; EE; ES; FI; GB; GD; GE; GH; GM; HR; HU; ID; IL; IN; IS; JP; KE; KG; KP; KR; KZ; LC; LK; LR; LS; LT; LU; LV; MA; MD; MG; MK; MN; MW; MX; MZ; NI; NO; NZ; OM; PH; PL; PT; RO; RU; SC; SD; SE; SG; SK; SL; TJ; TM; TN; TR; TT; TZ; UA; UG; US; UZ; VC; VN; YU; ZA; ZM; ZW;
DR: AT; BE; BG; CH; CY; CZ; DE; DK; EA; EE; ES; FI; FR; GB; GH; GM; GR; HU; IE; IT; KE; LS; LU; MC; MW; MZ; NL; OA; PT; SD; SE; SI; SK; SL; SZ; TR; TZ; UG; ZM; ZW;
IC: G06F-001/00; H04L-009/32; H04L-012/16; H04L-029/06;
MC: T01-N01A2A; T01-N02B1; T01-S03;
DC: T01;
FN: 2003833818.gif
PR: DE1015746 10.04.2002;
FP: 23.10.2003
UP: 08.06.2004


A
Agentenserver User (U1)
Ticket Granting Server (TGS)
0
105
106
1
2
4
3
102
Agent (A1)
B Ticket
Dienst (TD1)
107
103
5
104
6
101
Agent (A1)
C Server
Dienst (SD)
Agentenserver (S)
D
100

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 102 15 746 A 1**

(51) Int. Cl.[7]:
H 04 L 9/32
H 04 L 12/16

(21) Aktenzeichen: 102 15 746.4
(22) Anmeldetag: 10. 4. 2002
(43) Offenlegungstag: 6. 11. 2003

(71) Anmelder:
Siemens AG, 80333 München, DE

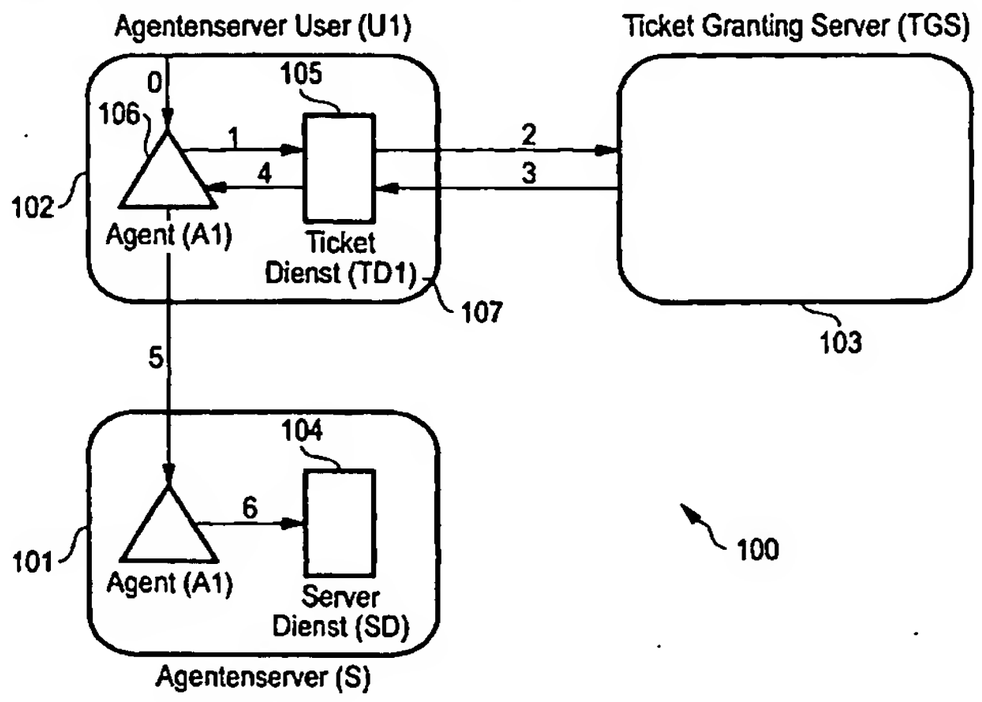
(72) Erfinder:
Fischer, Kai, 81673 München, DE; Lotz, Volkmar, 80639 München, DE; Waidelich, Fabienne, Dr., 80639 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Anordnung sowie Computerprogramm mit Programmcode-Mitteln und Computerprogramm-Produkt zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz

(57) Die Erfindung betrifft eine Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst. Dabei wird an eine Autorisierungsinstanz in dem Kommunikationsnetz eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst gestellt. Die Autorisierungsanfrage wird von der Autorisierungsinstanz überprüft. Anschließend werden Autorisierungsdaten dann von der Autorisierungsinstanz erzeugt, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst anzeigt, welche Autorisierungsdaten den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist.



DE 102 15 746 A 1

Beschreibung

[0001] Die Erfindung betrifft eine Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst.

[0002] Mobile Agenten sind aus [1] bekannt.

[0003] Mobile Agenten sind selbstständig agierende Computerprogramme, die autonom, zielgerichtet und arbeitsteilig im Auftrag einer Person oder Organisation (Autorität) Aufträge ausführen. Dabei sind sie autorisiert, in Namen der Autorität Entscheidungen zu treffen.

[0004] Mobile Agenten sind mobil, d. h. sie können während ihrer Lebenszyklen ihre jeweilige Ausführungsumgebung ändern, beispielsweise dadurch, dass sie in Kommunikationsnetzen von einem Kommunikationsgerät zu einem zweiten Kommunikationsgerät migrieren.

[0005] Mobile Agenten werden von Agentenplattformen bzw. in Agentensystemen erzeugt, welche neben der Agentenerzeugung die Agenten interpretieren, ausführen, übertragen und terminieren sowie Verbindungen zwischen Autoritäten und Agenten sowie zwischen Agenten herstellen.

[0006] Ferner werden von Agentenplattformen und/oder in Agentensystemen Dienste für die Autoritäten bzw. für die die Autoritäten vertretenden Agenten angeboten, wie Informationsdienste, elektronische Marktplätze oder elektronische Finanzdienstleistungen.

[0007] Diese Dienste sind einerseits öffentlich zugänglich, d. h. alle Autoritäten können diese Dienste mittels der sie vertretenden Agenten in Anspruch nehmen.

[0008] Andererseits werden auch Dienste angeboten, die nur einer geschlossenen Benutzergruppe, d. h. nur entsprechend berechtigten Autoritäten bzw. deren Agenten, zugänglich sind.

[0009] Für den Zugriff auf solche meist kostenpflichtigen, geschützten Dienste müssen die Agenten als Stellvertreter ihrer Autoritäten autorisiert werden.

[0010] Bei der Autorisierung eines Agenten wird zwischen einer grob granularen und einer fein granularen Autorisierung unterschieden.

[0011] Unter fein granular ist eine Einschränkung der Zugriffsrechte der Agenten auf die Dienste im Hinblick auf z. B. Umfang, Zeitdauer, Zeitpunkt und/oder Funktionalität zu verstehen. Dadurch, dass ein Agent bei der fein granularen Autorisierung nur solche Zugriffsrechte erhält bzw. nur für solche Zugriffsrechte autorisiert wird, welche für die auf ihn übertragene Aufgabe notwendig sind, wird ein möglicher Missbrauch von Agenten für andere Aufgaben eingeschränkt.

[0012] Im Gegensatz dazu erhält ein Agent bei einer grob granularen Autorisierung Zugriffsrechte uneingeschränkt.

[0013] Eine grob granulare Autorisierung ist aus [2], einer Agentenplattform SeMoA®, bekannt.

[0014] Bei der Agentenplattform SeMoA® authentifizieren sich Agenten durch eine eindeutige und nicht manipulierbare ID. Solche IDs sind durch kryptographische Verfahren direkt an die Autoritäten der Agenten gebunden, d. h. ein Agent verfügt über die gesamte Rechtemenge seiner jeweiligen Autorität.

[0015] Aus [3], einer Agentenplattform Ajanta, ist eine fein granulare Autorisierung bekannt.

[0016] Bei der Agentenplattform Ajanta erfolgt die fein granulare Autorisierung eines Agenten durch die entsprechende Autorität des Agenten selbst, was einen sogenannten, zusätzlichen Policy-Abgleich, d. h. eine Überprüfung der Zugriffsrechte unter übergeordneten Gesichtspunkten (Policy), beim Dienstanbieter erfordert.

[0017] Darüber hinaus wird durch diese Vorgehensweise der Autorisierung bei [3] eine Übertragung von Rechten von einem autorisierten Agenten auf einen anderen Agenten (Delegation) erschwert, weil dabei sogenannte Attributsketten, auch bekannt aus [6], welche die Übertragung nachzeichnen, zu bilden sind.

[0018] Eine Delegation ermöglicht, Teilaufgaben auch von zweiten Agenten, welche im Auftrag der ursprünglich autorisierten, ersten Agenten handeln, ausführen zu lassen. Diese zweiten Agenten können auch Agenten anderer Autoritäten sein.

[0019] Zu berücksichtigende Sicherheitsaspekte bei den mobilen Agenten erfordern außerdem, dass mobile Agenten kein privates bzw. geheimes Schlüsselmaterial mit sich führen dürfen. Sie sind somit nicht in der Lage, auf entfernten Agentenplattformen kryptographische Operationen mit solchen Schlüsseln durchzuführen.

[0020] Aus [4] ist eine Autorisierung, ein sogenannter "Kerberos Network Authentication Service", zur Autorisierung eines Client durch einen Server in einer Client/Server-Umgebung bekannt.

[0021] Die Autorisierung bei dem "Kerberos Network Authentication Service" erfolgt unter Verwendung von Authentifikations- und Autorisierungsprotokollen und beruht darauf, dass eine kryptographische Operation mit privaten bzw. geheimen Schlüsseln notwendig ist.

[0022] Somit liegt der Erfindung die Aufgabe zugrunde, eine fein granulare und aufgabenspezifische Autorisierung eines Agenten auf einfache Weise zu ermöglichen. Darüber hinaus soll die Erfindung es ermöglichen, auf einfache Weise Zugriffsrechte von einem ersten Agenten auf einen zweiten Agenten zu delegieren.

[0023] Diese Aufgaben werden durch das Verfahren und die Anordnung sowie durch das Computerprogramm mit Programmcode-Mitteln und das Computerprogramm-Produkt zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz mit den Merkmalen gemäß dem jeweiligen unabhängigen Patentanspruch gelöst.

[0024] Bei dem Verfahren zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst werden

a) an eine Autorisierungsinstanz in dem Kommunikationsnetz eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst gestellt,
b) die Autorisierungsanfrage von der Autorisierungsinstanz überprüft und
c) Autorisierungsdaten dann von der Autorisierungsinstanz erzeugt, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst anzeigt, welche Autorisierungsdaten den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist.

[0025] Die Anordnung zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst ist derart eingerichtet, dass

- an sie eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst stellbar ist,
- durch sie die Autorisierungsanfrage überprüfbar ist und dann, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst anzeigt, Autorisierungsdaten erzeugbar sind, welche den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist.

[0026] Das Computerprogramm mit Programmcode-Mitteln ist eingerichtet, um alle Schritte gemäß dem erfindungs-

gemäßen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

[0027] Das Computerprogramm-Produkt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode-Mitteln ist eingerichtet, um alle Schritte gemäß dem erfindungsgemäßen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

[0028] Die Anordnung sowie das Computerprogramm mit Programmcode-Mitteln, eingerichtet um alle Schritte gemäß dem erfinderischen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird, sowie das Computerprogramm-Produkt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode-Mitteln, eingerichtet um alle Schritte gemäß dem erfinderischen Verfahren durchzuführen, wenn das Programm auf einem Computer ausgeführt wird, sind insbesondere geeignet zur Durchführung des erfindungsgemäßen Verfahrens oder einer seiner nachfolgend erläuterten Weiterbildungen.

[0029] Der Erfindung liegt der Grundgedanke zugrunde, Prinzipien des Client/Server-Umfelds in nicht trivialer Weise in einen Kontext mobiler Agentensysteme zu portieren, diese entsprechend dem neuen Umfeld anzupassen und dabei bei mobilen Agentensystemen vorhandene Mechanismen von Agentenplattformen, wie Authentifikationsverfahren zur eindeutigen und nicht manipulierbaren Authentifikation von mobilen Agenten, in nicht trivialer Weise mit den Prinzipien zu kombinieren und sie zu nutzen.

[0030] Dabei ist ein grundlegender Gedanke der Erfindung, die Autorisierung von Agenten durch sogenannte Autorisierungsdaten zu realisieren. Diese werden bei der Erfindung von einer zentralen Instanz, der Autorisierungsinstanz, ausgestellt und sind auf eindeutige Weise dem jeweiligen Agenten zugeordnet.

[0031] Die Autorisierungsdaten enthalten die Informationen für die fein granulare und aufgabenspezifische Autorisierung, wobei auch übergeordnete, globale Gesichtpunkte, eine sogenannte Policy, zentral berücksichtigt werden kann.

[0032] Gerade dadurch, dass die Autorisierungsdaten von einer zentralen Instanz und eben nicht lokal ausgestellt werden, d. h. von einer Autorität, welche den mobilen Agenten in der Regel erzeugt, können zentral bzw. auf übergeordneter Ebene globale Gesichtspunkte bzw. Randbedingungen (Policy), wie bestimmte globale Einschränkungen von Zugriffsrechten, berücksichtigt werden.

[0033] Agenten erhalten somit bei der Erfindung in Form der jeweiligen Autorisierungsdaten nur diejenigen Rechte, die tatsächlich zur Ausführung der an sie gestellten Aufgabe notwendig sind.

[0034] Durch diesen Ansatz wird die Möglichkeit minimiert, dass ein Agent eine andere als diejenige durchführt, für die er von seiner Autorität instruiert wurde.

[0035] Weiterhin ermöglich die Erfindung, dass Agenten ihre Rechte oder auch nur eine Teilmenge ihrer Rechte an andere Agenten delegieren können. Rechte können sowohl an Agenten derselben Autorität als auch an Agenten anderer Autoritäten delegiert werden.

[0036] Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

[0037] Die im weiteren beschriebenen Weiterbildungen beziehen sich sowohl auf die Verfahren als auch auf die Anordnung.

[0038] Die Erfindung und die im weiteren beschriebenen Weiterbildungen können sowohl in Software als auch in Hardware, beispielsweise unter Verwendung einer speziellen elektrischen Schaltung, realisiert werden.

[0039] Ferner ist eine Realisierung der Erfindung oder einer im weiteren beschriebenen Weiterbildung möglich durch ein computerlesbares Speichermedium, auf welchem das Computerprogramm mit Programmcode-Mitteln gespeichert ist, welches die Erfindung oder Weiterbildung ausführt.

[0040] Auch kann die Erfindung oder jede im weiteren beschriebene Weiterbildung durch ein Computerprogrammerzeugnis realisiert sein, welches ein Speichermedium aufweist, auf welchem das Computerprogramm mit Programmcode-Mitteln gespeichert ist, welches die Erfindung oder Weiterbildung ausführt.

[0041] Zur Spezifizierung der Autorisierung des mobilen Agenten ist es zweckmäßig, dass die Autorisierungsdaten mindestens eine der folgenden Informationen enthalten:

- eine Gültigkeitsdauer, wie lange die Autorisierung gültig ist,
- eine Autorisierungsinformation, welche den Dienst kennzeichnet, insbesondere einen Umfang des Dienstes, einen Anbieter des Dienstes, eine Lokalisierungsinformation des Anbieters des Dienstes,
- eine Agenteninformation, welche den mobilen Agenten, welcher für den Dienst autorisiert wurde, bezeichnet (Agenten-ID).

[0042] Derartige Autorisierungsdaten ermöglichen eine eindeutige Verknüpfung zwischen klar definierten Zugriffsrechten und dem entsprechend autorisierten mobilen Agenten. Dadurch werden Manipulationsmöglichkeiten eingeschränkt.

[0043] Ferner kann die Sicherheit vor Manipulation und Missbrauch auch dadurch erhöht werden, dass die Autorisierungsanfrage und/oder die Autorisierungsdaten unter Verwendung eines kryptographischen Verfahrens/kryptischer Verfahren, wie eine digitale Signatur, geschützt werden. Verwendbare kryptographische Verfahren sind in [5] beschrieben.

[0044] Des weiteren ist es sinnvoll, eine Kommunikation bzw. einen Datenaustausch zwischen der Autorisierungsinstanz und dem mobilen Agenten durch einen Ticketdienst abzuwickeln. Dadurch lassen sich einzelne klar strukturierte, funktionelle Module bzw. Komponenten, beispielsweise durch entsprechend eingerichtete Server, realisieren.

[0045] So wäre dementsprechend die Funktion eines solchen Ticketdienstes das Stellen der Anfrage an die Autorisierungsinstanz, das Empfangen und Weiterreichen der Autorisierungsdaten an den mobilen Agenten. Auch zusätzliche Aufgaben bei Agentenplattformen und/oder Agentensystemen kann ein solcher Ticketdienst übernehmen, wie eine Authentifikationsprüfung des mobilen Agenten und/oder eine Authentifikationsprüfung der Autorisierungsinstanz.

[0046] Auch ist es möglich, den Ticketdienst und die Authorisierungsinstanz in einer Instanz zu integrieren.

[0047] Auch ist es sinnvoll, die Autorisierungsdaten in einem Ticket zusammenzufassen. Grundzüge einer Tickettechnik sind aus [4] bekannt.

[0048] Das Ticket kann durch kryptographische Verfahren [5] vor Missbrauch und Manipulationen geschützt werden. Eine Verknüpfung des auf einen mobilen Agenten ausgestellten Tickets mit diesem wird durch die Authentifikation des mobilen Agenten gewährleistet.

[0049] Ist nun der mobile Agent mit dem Ticket ausgestattet, so migriert er innerhalb des Kommunikationsnetzes, dorthin, wo der von ihm nachzufragende Dienst, beispielsweise ein Reisedienst oder ein Einkaufsdienst, bzw. der entsprechende Dienstanbieter lokalisiert ist. Dort wird der mobile Agent authentifiziert. Beim Versuch des Zugriffs auf den Dienst muss der mobile Agent seine Legitimation beweisen, was durch Übergabe des Tickets an den Dienstanbieter und die Überprüfung des Tickets und der dort nieder-

gelegten Berechtigung durch den Dienstanbieter erfolgt.

[0050] In einem solchen Rechnernetz sind in der Regel der Dienstanbieter, die Autorisierungsinstanz sowie der Tikketdienst durch Server realisiert.

[0051] Ein mobile Agent selbst wird in der Regel dann erzeugt, wenn ein Kommunikationsteilnehmer in dem Kommunikationsnetz einen dort angebotenen Dienst in Anspruch nehmen möchte.

[0052] In einer Weiterbildung stellt der mobile Agent die Autorisierungsanfrage für sich selbst, d. h. er selbst möchte auf ihn ausgestellte und ihn autorisierende Autorisierungsdaten haben.

[0053] Alternativ ist es auch möglich, dass ein anderer, zweiter autorisierter mobiler Agent die Autorisierungsanfrage für den ersten mobilen Agenten stellt. Die Autorisierungsdaten werden dann auf Basis der Autorisierung des anderen, zweiten mobilen Agenten für den ersten mobilen Agenten ausgestellt. Der erste mobile Agent erhält anschließend direkt oder indirekt von dem anderen, zweiten mobilen Agenten die auf ihn ausgestellten Autorisierungsdaten.

[0054] Diese Vorgehensweise eignet sich insbesondere zu einer Übertragung von Autorisierungen, was als Delegation bezeichnet wird.

[0055] In diesem Fall wäre bei obiger Vorgehensweise der andere, zweite mobile Agent ein sogenannter Delegationsagent. Er delegiert seine ursprüngliche Autorisierung, d. h. seine ursprünglichen Rechte, an den ersten mobilen Agenten.

[0056] Im Detail kann eine solche Delegation derart realisiert werden:

- der Delegationsagent ist durch ursprüngliche Autorisierungsdaten ursprünglich für den Dienst autorisiert,
- der Delegationsagent stellt die Autorisierungsanfrage für den mobilen Agenten, durch welche die Autorisierungsdaten für den mobilen Agenten unter Verwendung der ursprünglichen Autorisierungsdaten erzeugt werden,
- der mobile Agent wird mit den Autorisierungsdaten ausgestattet, wobei die ursprünglichen Autorisierung des Delegationsagenten auf den mobilen Agenten übertragen wird.

[0057] In Figuren sind Ausführungsbeispiele der Erfindung dargestellt, welche im weiteren näher erläutert werden.

[0058] Es zeigen

[0059] **Fig.** 1 Autorisierung eines mobilen Agenten gemäß einem ersten Ausführungsbeispiel;

[0060] **Fig.** 2 Autorisierung eines zweiten mobilen Agenten durch Übertragung einer Autorisierung von einem ersten autorisierten Agenten auf den zweiten mobilen Agenten gemäß einem zweiten Ausführungsbeispiel.

[0061] Erstes Ausführungsbeispiel: Autorisierung eines mobilen Agenten in einem Agentensystem In **Fig.** 1 ist ein Ausschnitt eines Rechnernetzes **100** mit mehreren miteinander vernetzten Servern **101, 102, 103**, auf welchen ein Agentensystem mit entsprechend eingerichteten Agentenplattformen implementiert ist, dargestellt.

[0062] Grundlegende Netz- und Servertechniken sowie Agentenplattformen sind allgemein bekannt.

[0063] **Fig.** 1 zeigt einen Server **101** eines Dienstanbieters S (Agentenserver S 101), welcher einen zugangsbeschränkten und kostenpflichtigen Dienst SD **104**, in diesem Fall einen Reisebuchungsdienst, anbietet.

[0064] **Fig.** 1 zeigt ferner einen Server **102** (Agentenserver User U1 102) eines Benutzers U1 (User U1). Auf dem Agentenserver User U1 102 ist ein Ticket Dienst (TD1) **107**, ein entsprechend programmiertes Computerprogramm, implementiert, mittels welchem Zugriffsrechte in Form von sogenannten Tickets **105** auf Dienste in dem Rechnernetz **100** erlangbar sind.

[0065] Auch zeigt **Fig.** 1 einen Ticket Granting Server **103**, welcher Autorisierungszertifikate, die sogenannten Tickets **105**, für mobile Agenten des Agentensystems, wie Agent A1 106, ausstellt.

[0066] Grundzüge einer Tickettechnik sind in [4] beschrieben.

[0067] Ein von dem Ticket Granting Server **103** ausgestelltes Ticket **105** ist auf eindeutige Weise demjenigen Agenten, beispielsweise dem Agenten A1 106, zugeordnet, für den es ausgestellt wird. Es definiert das dem Agenten zugestandene Recht. Dazu enthält das Ticket **105** entsprechende Autorisierungsdaten. Die Autorisierungsdaten setzen sich zusammen aus einer Agenten ID, einer Gültigkeitsdauer des Tickes **105**, einer Angabe, wo und wie es einzulösen ist, sowie aus einer Beschreibung des konkreten zugestandene Rechts.

[0068] Das Ticket **105** ist darüber hinaus durch eine digitale Signatur vor Missbrauch und Manipulationen geschützt.

[0069] In **Fig.** 1 dargestellte Pfeile 0 bis 6 kennzeichnen die bei einer Nachfrage nach dem Dienstes SD **104** ablaufenden Schritte 0 bis 6.

0. Der User (U1) möchte eine Reise buchen und will dazu den Dienst (SD) **104** im Rechnernetz **100** in Anspruch nehmen. Er greift über seinem Agentenserver User (U1) **192** auf den Dienst (SD) **104** des Agentenservers (S) **101** zu und startet bzw. erzeugt hierfür auf seiner Agentenplattform den Agenten (A1), der als Stellvertreter von U1 agiert.
Da der Dienst (SD) **104** zugangsbeschränkt, weil kostenpflichtig, ist, muss der Agent A1 106 entsprechend autorisiert sein.

1. Der Agent A1 106 fordert bei dem Ticket-Dienst (TD1) **107** des Agentenserver User (U1) **102** ein Ticket (T1) **105** für den Zugriff auf den Dienst SD **104** an. Der Ticket-Dienst TD1 107 ermittelt die eindeutige Identität von A1.

2. Ticket-Dienst TDI **107** fordert bei einer zentralen Instanz, dem Ticket-Granting-Server (TGS) **103**, das Ticket **105** für den Agenten A1 106 an (Ticket Request).
Hierfür wird dem Ticket-Granting-Server (TGS) **103** die eindeutige Identität vom Agenten A1 106 mitgeteilt. Auch die Authentizität des Users U1 wird überprüft.
Anschließend prüft der Ticket-Granting-Server (TGS) **103** anhand von gespeicherten Benutzerrechten, welche Rechte er dem Agenten A1 106 als Stellvertreter des Users U1 ausstellen darf und gleicht diese mit seiner übergeordneten Policy ab. Dann stellt er das entsprechende Ticket **105** für den Agenten A1 106 aus.
Der Ticket-Request ist durch kryptographische Operationen geschützt.

3. Der Ticket-Granting-Server (TGS) **103** übergibt das für den Agenten A1 106 ausgestellte Ticket **105** an den Ticket-Dienst TD1 107 (Ticket Reply).
Der Ticket-Reply ist ebenfalls durch kryptographische Operationen geschützt. Die Authentizität von TGS **103** wird ebenfalls überprüft.

4. Der Agent A1 106 bekommt vom Ticket-Dienst TD1 107 das Ticket **105**.

5. Der Agent A1 106 migriert zum Agentenserver S 101. Beim Betreten der Agentenplattform des Agentenservers S 101 wird der Agent A1 106 eindeutig und nicht manipulierbar authentifiziert.

6. Der Agent A1 106 möchte auf den Dienst SD **104** zugreifen und übergibt das Ticket **105**. Der Dienst SD **104** überprüft die Gültigkeit des Tickets **105** und führt den Zugriff gemäß den im Ticket **105** gespeicherten Rechten aus.

[0070] Zweites Ausführungsbeispiel: Autorisierung eines mobilen Agenten A2 durch Delegation durch den mobilen Agenten A1 106 in dem Agentensystem (**Fig.** 2)

[0071] Das zweite Ausführungsbeispiel beschreibt zusammen mit **Fig.** 2 eine Delegation eines zweiten mobilen Agenten A2 201 durch den mobilen Agenten A1 106.

[0072] Ohne Beschränkung der Allgemeinheit ist der zweite Agent A2 201 einem anderen Benutzer als User U1 zugehörig.

[0073] Die in **Fig.** 2 dargestellten Pfeile **1** bis **8** kennzeichnen die bei der Delegation (der Nachfrage nach dem Dienstes SD **104**) ablaufenden Schritte **1** bis **8**.

[0074] Ausgangssituation bei der nachfolgend beschriebenen Delegation ist, dass der Agent A1 106 im Besitz des auf ihn ausgestellten Tickets **105** ist. Des weiteren befindet sich der Agent A1 106 auf der Agentenplattform des Agentenservers S 101. Auf dieses befindet sich ebenfalls der Agent A2 201.

1. Agent A1 106 migriert zum Agentenserver User U1 102. Beim Betreten der Agentenplattform wird der Agent A1 106 eindeutig und nicht manipulierbar authentifiziert.
2. Der Agent A1 106 fordert beim Ticket-Dienst TD1 107 ein Ticket (T2) **202** für den Agenten A2 201 an. Der Ticket-Dienst TD1 107 ermittelt die eindeutige Identität vom Agenten A1 106.
3. Der Ticket-Dienst TDI **107** fordert bei dem Ticket-Granting-Server (TGS) **103** das Ticket **202** für den Agenten A2 201 an Ticket Request).
Hierfür wird dem Ticket Granting Server TGS **103** die eindeutige Identität von Agent A1 106 und von Agent A2 201 mitgeteilt. Auch die Authentizität des Users U1 wird wieder überprüft.
Der Ticket Granting Server TGS **103** prüft dann in analoger Weise wie zuvor beim Agenten A1 106, welche Rechte dem Agenten A2 202 zugestanden werden können.
Das Ticket **105** von Agent A1 106 wird als Basis für das Ticket **202** von Agent A2 201 herangezogen.
Der Ticket-Request ist durch kryptographische Operationen geschützt.
4. Der Ticket Granting Server TGS **103** übergibt das für den Agenten A2 201 ausgestellte Ticket **202** an den Ticket Dienst TDI **107** (Ticket Reply).
Der Ticket-Reply ist ebenfalls durch kryptographische Operationen geschützt. Auch die Authentizität des Tikket Granting Servers TGS **103** wird überprüft.
5. Der Agent A1 106 bekommt vom Ticket-Dienst TDI **107** das Ticket **202**.
6. Der Agent A1 106 migriert zum Agentenserver S 101. Beim Betreten der Agentenplattform des Agentenservers S 101 wird der Agent A1 106 eindeutig und nicht manipulierbar authentifiziert.
7. Der Agent A1 106 übergibt das Ticket **201** an den Agenten A2 201.
8. Der Agent A2 201 greift auf den Dienst SD **104** zu und übergibt das Ticket **202**. Der Dienst SD **104** überprüft die Gültigkeit des Tickets **202** und führt den Zugriff gemäß den im Ticket **202** gespeicherten Rechten aus.

[0075] In diesem Dokument sind folgende Schriften zitiert:

[1] M. N. Huhns, M. P. Singh; Readings in Agents; Morgan Kaufmann Publishers Inc., 1998;
[2] Agentenplattform SeMoA©, erhältlich am 23.03.2002 unter: http:// www.semoa.org
[3] Agentenplattform Ajanta, in "Delegation of Privileges to Mobile Agents in Ajanta", erhältlich am 23.03.2002 unter: http:// www.cs.umn.edu/Ajanta/papers/ic2000.pdf;
[4] Kerberos (IETF RFC **1510**);
[5] Bruce Schneider; Applied Cryptography; Second Edition; John Wiley & Sons, Inc.;
[6] SPKI-Attributszertifikate (IETF RFC2692, IETF RFC2693).

Patentansprüche

1. Verfahren zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst, bei dem
a) an eine Autorisierungsinstanz in dem Kommunikationsnetz eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst gestellt wird,
b) die Autorisierungsinstanz die Autorisierungsanfrage überprüft und
c) die Autorisierungsinstanz, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst (bzw. mindestens eines Teils des Dienstes) anzeigt, Autorisierungsdaten erzeugt, welche den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist, andernfalls die Autorisierungsinstanz keine Autorisierungsdaten erzeugt.
2. Verfahren nach Anspruch 1, bei dem die Autorisierungsdaten mindestens eine der folgenden Informationen enthalten:
– eine Gültigkeitsdauer, wie lange die Autorisierung gültig ist,
– eine Autorisierungsinformation, welche den Dienst kennzeichnet, insbesondere einen Umfang des Dienstes, einen Anbieter des Dienstes, eine Lokalisierungsinformation des Anbieters des Dienstes,
– eine Agenteninformation, welche den mobilen Agenten, welcher für den Dienst autorisiert wurde, bezeichnet (Agenten-ID).
3. Verfahren nach Anspruch 1 oder 2, bei dem die Autorisierungsanfrage und/oder die Autorisierungsdaten unter Verwendung eines kryptographischen Verfahrens/kryptischer Verfahren geschützt werden.
4. Verfahren nach Anspruch 3, bei dem die Autorisierungsdaten mit einer digitalen Signatur versehen werden.
5. Verfahren nach einem der vorangehenden Ansprüche, bei dem die Autorisierungsanfrage von einem Tikketdienst bei der Autorisierungsinstanz gestellt wird, welcher Ticketdienst den mobilen Agenten mit einem Ticket, welches die Autorisierungsdaten enthält, ausstattet.
6. Verfahren nach einem der vorangehenden Ansprüche, bei dem der Agent unter Verwendung der Autorisierungsdaten bei einem Dienstanbieter um den Dienst nachfragt.
7. Verfahren nach einem der vorangehenden Ansprüche, bei dem das Kommunikationsnetz ein verteiltes Rechnernetz ist, wobei die Autorisierungsinstanz ein Serverrechner in dem verteilten Rechnernetz ist.

8. Verfahren nach einem der vorangehenden Ansprüchen, bei dem ein Kommunikationsteilnehmer in dem Kommunikationsnetz den Dienst in Anspruch nehmen möchte und dabei den mobilen Agenten erzeugt.

9. Verfahren nach einem der vorangehenden Ansprüche, bei dem der mobile Agent die Autorisierungsanfrage stellt.

10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem ein Delegationsagent die Autorisierungsanfrage für den mobilen Agenten stellt.

11. Verfahren nach Anspruch 10, eingesetzt zur Übertragung einer ursprünglichen Autorisierung des Delegationsagenten für den Dienst auf den mobilen Agenten,
wobei der Delegationsagent durch ursprüngliche Autorisierungsdaten ursprünglich für den Dienst autorisiert war,
wobei der Delegationsagent die Autorisierungsanfrage für den mobilen Agenten stellt, durch welche die Autorisierungsdaten für den mobilen Agenten unter Verwendung der ursprünglichen Autorisierungsdaten erzeugt werden
und wobei der mobile Agent mit den Autorisierungsdaten ausgestattet wird, wobei die ursprünglichen Autorisierung des Delegationsagenten auf den mobilen Agenten übertragen wird.

12. Anordnung zur Autorisierung eines mobilen Agenten in einem Kommunikationsnetz für einen in dem Kommunikationsnetz angebotenen Dienst,
an welche Autorisierungsanordnung eine Autorisierungsanfrage zur Autorisierung des mobilen Agenten für den Dienst stellbar ist,
durch welche Autorisierungsanordnung die Autorisierungsanfrage überprüfbar ist und, wenn die Überprüfung eine Berechtigung des mobilen Agenten für den Dienst (bzw. mindestens eines Teils des Dienstes) anzeigt, Autorisierungsdaten erzeugbar sind, welche den mobilen Agenten für den Dienst autorisieren und mit welchen der mobile Agent ausstattbar ist, andernfalls keine Autorisierungsdaten erzeugbar sind.

13. Autorisierungsanordnung nach Anspruch 12, eingesetzt in einem Kommunikationsnetz zur Autorisierung des mobilen Agenten in einem Kommunikationsnetz für den in dem Kommunikationsnetz angebotenen Dienst.

14. Computerprogramm mit Programmcode-Mitteln, um alle Schritte gemäß Anspruch 1 durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

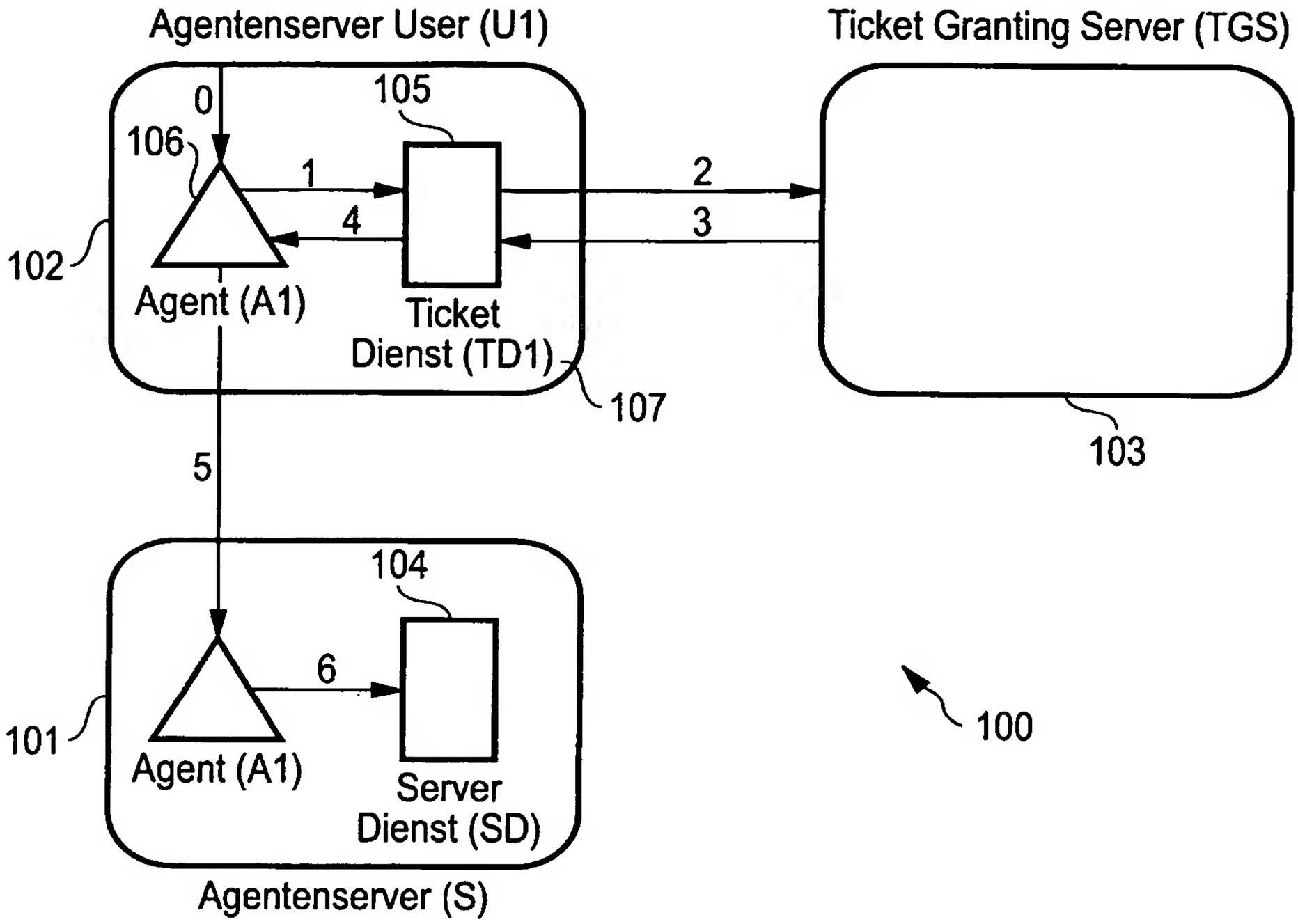
15. Computerprogramm mit Programmcode-Mitteln gemäß Anspruch 14, die auf einem computerlesbaren Datenträger gespeichert sind.

16. Computerprogramm-Produkt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode-Mitteln, um alle Schritte gemäß Anspruch 1 durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 102 15 746 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. November 2003

FIG 1



Nummer: DE 102 15 746 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 6. November 2003

FIG 2